INFOSECTRAIN

SOC ANALYST TRAINING

www.infosectrain.com | sales@infosectrain.com

Course Description

The SOC analyst training program is meticulously designed by the subject matter experts at Infosec Train. The training program offers a deep insight into the SOC operations and workflows. It is an excellent opportunity for aspiring and current SOC analysts (L1/L2/L3) to level up their skills to mitigate business risks by effectively handling and responding to security threats.

Objective

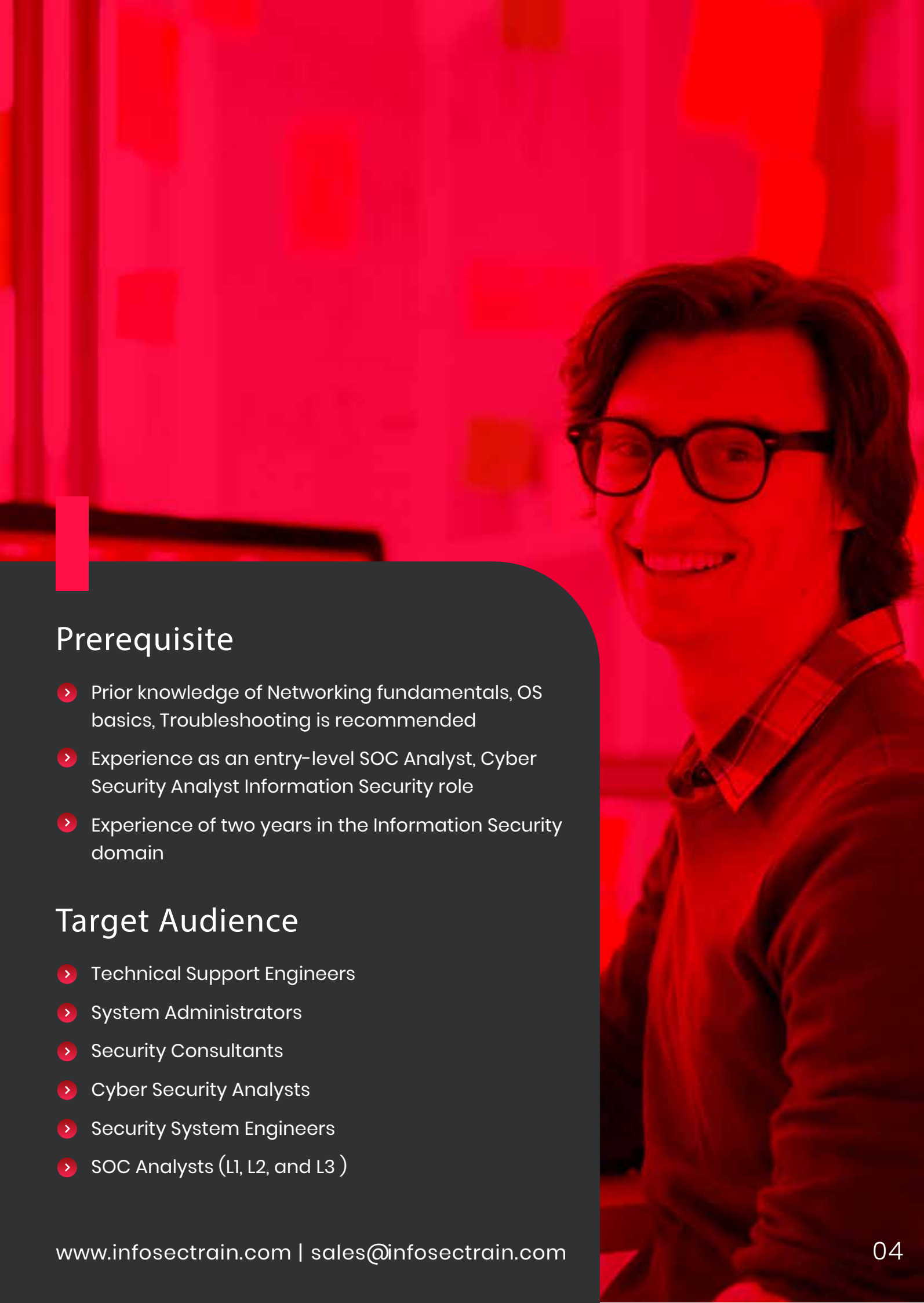
Our SOC Training Program will help you to master over trending and in-demand technical skills. The program starts with intermediate-level cybersecurity concepts and then proceeds to advanced forensic, threat Intelligence, Security incident, and Event Management Solutions. Infosec Train's SOC Training Course provides cybersecurity professionals with advanced security skills and certification. The training program will allow you to:

- Perform technical strategies, tools, and techniques to secure data for your organization.
- Understanding the threats and providing countermeasures.
- Understand network forensics and incident response in depth.
- Cybersecurity industry knowledge
- Analyze and Classify Malware

Why SOC Analyst with Infosec Train?

SOC Analyst Training serves as a launchpad for developing security professionals. Its demand is continuously increasing in the industry. The certified SOC analyst certification will not only enhance your knowledge on various SOC operations but will also:

- Help you to showcase your skills and working experience for the SOC Analyst job position
- Provide you opportunities to secure a job in the other network security-related domains
- Keep you updated with the latest skills necessary for L1/L2/L3 SOC Analyst job positions
- Enable you to demonstrate to employers that you are committed to professional growth and you are better equipped with skills to carry out complex tasks within the SOC team



Prerequisite

- Prior knowledge of Networking fundamentals, OS basics, Troubleshooting is recommended
- Experience as an entry-level SOC Analyst, Cyber Security Analyst Information Security role
- Experience of two years in the Information Security domain

Target Audience

- Technical Support Engineers
- System Administrators
- Security Consultants
- Cyber Security Analysts
- Security System Engineers
- SOC Analysts (L1, L2, and L3)

Domain 1: Security Operations Centre

Introduction to SOC

- Building a successful SOC
- Functions of SOC
- Heart of SOC- SIEM
- Gartner's magic quadrant
- SIEM guidelines and architecture

ELK Stack:

- Introduction and an overview of Elastic SIEM
- User interface
- How to as a part of alert investigations or interactive threat hunting
- MDR vs. Traditional SIEM; and other various solutions
- Elasticsearch: Understanding of Architecture, curator fundamentals
- Index template for routing, mapping
- KIBANA: Configuration, policies, visualization
- Deep-dive of Log architecture, parsing, alerts

SecurityOnion

- What is Security Onion?
- Monitoring and analysis tools
- Security Onion Architecture
- Deployment types
- Installing a Standalone server: checking system services with sostat, security onion with web browser tools, security onion terminal
- Replaying traffic on a standalone server

Splunk In-Depth

- Industrial requirements of Splunk in various fields
- Splunk terminologies, search processing language, and various industry use cases

AlienVault OSSIM fundamentals

- AlienVault fundamentals and architecture deployment
- Vulnerability scanning & monitoring with OSSIM

Introduction to QRadar

- IBM QRadar SIEM component architecture and data flows
- Using the QRadar SIEM User Interface

Fun with logs

- Working with offense triggered by events
- Working with offense triggered by flows

Monitoring

- Monitor QRadar Notifications and error messages.
- Monitor QRadar performance
- Review and interpret system monitoring dashboards.
- Investigate suspected attacks and policy breaches
- Search, filter, group, and analyze security data

Tools exposure provided in the above section:

- SecurityOnion
- ELK Stack
- SGUILD
- Wireshark
- Splunk
- AlienVault OSSIM
- IBM Qradar CE

Domain 2: Digital Forensics

1: Introduction to Digital Forensics

- Section Introduction
- What is Digital Forensics?
  - Collecting evidence typically related to cybercrime
- Digital Subject Access Requests
- Computer Forensics Process
  - Identification, Preservation, collection, examination, analysis, reporting
- Working with Law Enforcement
  - The difference between an internal security issue and one that requires external assistance

2: Forensics Fundamentals Section Introduction

- Introduction to Data Representation

hexadecimal, octal, binary files vs. txt files, timestamp formats: UNIX epoch, MAC, Chrome, Windows, FILETIME

- Hard Drive Basics
  - Platters, sectors, clusters, slack space
- SSD Drive Basics
  - garbage, collection, TRIM, wear leveling
- File Systems
  - FAT16, FAT32, NTFS, EXT3/EXT4, HFS+/APFS
- Metadata & File Carving
- Memory, Page File, and Hibernation File
- Order of Volatility

3: Evidence Forms

• Section Introduction

• Volatile Evidence

- Memory RAM, Cache, Registers content, Routing tables, ARP cache, process table, kernel statistics, temporary file

system/swap space

• Disk Evidence

- Data on Hard Disk or SSD

• Network Evidence

- Remotely Logged Data, Network Connections/Netflow, PCAPs, Proxy logs

• Web & Cloud Evidence

- Cloud storage/backups, chat rooms, forums, social media posts, blog posts

• Evidence Forms

- Laptops, desktops, phones, hard drives, tablets, digital cameras, smartwatches, GPS

4: Chain of Custody

• Section Introduction

• What is the Chain of Custody?

• Why is it Important?

- In regard to evidence integrity and examiner authenticity

• Guide for Following the Chain of Custody

- evidence collection, reporting/documentation, evidence hashing, write-blockers, working on a copy of original evidence

5: Windows Investigations

• Section Introduction

• Artifacts

- Registry, Event Logs, Prefetch, .LNK files, DLLs, services, drivers, common malicious locations, schedules tasks, start-up files

• Limitations

• Example Investigations

6: *nix Investigations

• Section Introduction
• Artefacts
• Limitations
• Example Investigations
• Artefact Collection
  - Section Introduction
  - Equipment
  - non-static bags, faraday cage, labels, clean hard drives, forensic workstations, Disk imagers, hardware write blockers, cabling, blank media, photographs
  - Tools
  - Wireshark, Network Miner, and others
  - ACPO Principles
  - Live Forensics
  - Fast acquisition of key files
  - How to Collect Evidence
  - Laptops, desktops, phones, hard drives, tablets, websites, forum posts, blog posts, social media posts, chat rooms
  - Types of Hard Drive Copies visible data, bit for bit, slackspace

7: Live Forensics

• Section Introduction
• Live Acquisition
  - What is a live acquisition/live forensics? Why is it beneficial?
• Products
  - Carbon Black, Encase, memory analysis with agents, Custom Scripts
• Potential Consequences
  - Damaging or modifying evidence making it invalid

8: Post-Investigation

• Section Introduction
• Report Writing
• Evidence Retention
  - Legal retention periods, internal retention periods
• Evidence Destruction
  - Overwriting, degaussing, shredding, wiping
  - Further Reading

9: Tools exposure provided in the above section:

• Command-LINE for Windows / Linux
• FTK IMAGER
• MAGNATE RAM CAPTURE
• AUTOPSY
• Volatility
• Volatility WorkBench
• ENCASE

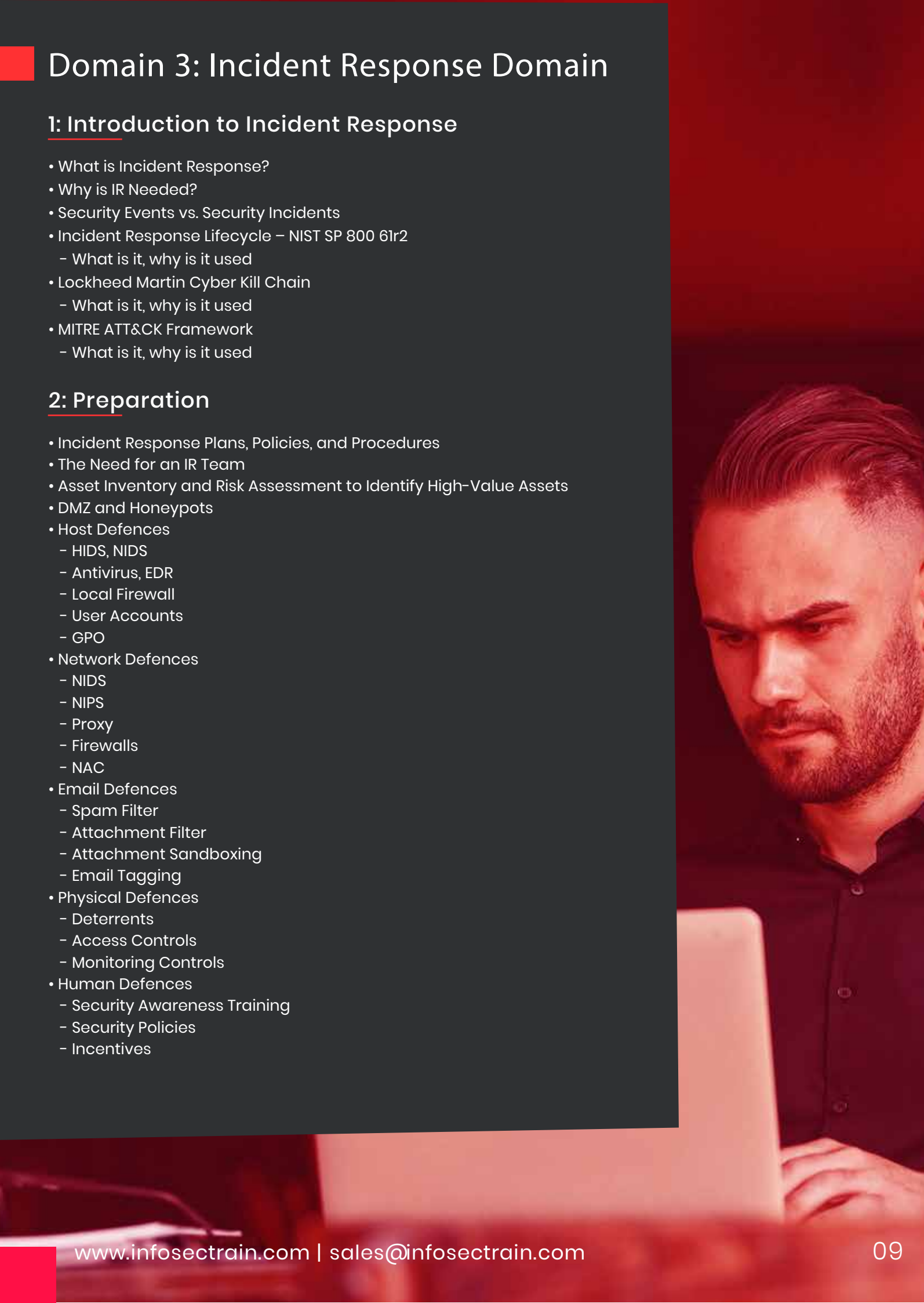
Domain 3: Incident Response Domain

1: Introduction to Incident Response

- What is Incident Response?
- Why is IR Needed?
- Security Events vs. Security Incidents
- Incident Response Lifecycle – NIST SP 800 61r2
  - What is it, why is it used
- Lockheed Martin Cyber Kill Chain
  - What is it, why is it used
- MITRE ATT&CK Framework
  - What is it, why is it used

2: Preparation

- Incident Response Plans, Policies, and Procedures
- The Need for an IR Team
- Asset Inventory and Risk Assessment to Identify High-Value Assets
- DMZ and Honeypots
- Host Defences
  - HIDS, NIDS
  - Antivirus, EDR
  - Local Firewall
  - User Accounts
  - GPO
- Network Defences
  - NIDS
  - NIPS
  - Proxy
  - Firewalls
  - NAC
- Email Defences
  - Spam Filter
  - Attachment Filter
  - Attachment Sandboxing
  - Email Tagging
- Physical Defences
  - Deterrents
  - Access Controls
  - Monitoring Controls
- Human Defences
  - Security Awareness Training
  - Security Policies
  - Incentives



3: Detection and Analysis

- Common Events and Incidents
- Establishing Baselines and Behaviour Profiles
- Central Logging (SIEM Aggregation)
- Analysis (SIEM Correlation)

4: Containment, Eradication, Recovery

- CSIRT and CERT Explained
  - What are they, and why are they useful?
- Containment Measures
  - Network Isolation, Single VLAN, Powering System(s) Down, Honeypot Lure
- Taking Forensic Images of Affected Hosts
  - Linking Back to Digital Forensics Domain
- Identifying and Removing Malicious Artefacts
  - Memory and disk analysis to identify artefacts and securely remove them
- Identifying Root Cause and Recovery Measures

5: Lessons Learned

- What Went Well?
  - Highlights from the Incident Response
- What Could be Improved?
  - Issues from the Incident Response, and How These Can be Addressed
- Important of Documentation
  - Creating Runbooks for Future Similar Incidents, Audit Trail
- Metrics and Reporting
  - Presenting Data in Metric Form
- Further Reading

6: Tools exposure provided in the above section:

- SYSINTERNAL SUITE
- Hash Calculator
- Online Sources
- CyberChef
- Wireshark
- Network Minor

Domain 4: Threat Intelligence Domain

1: Introduction to Incident Response

• Section Introduction
• Threat Intelligence Explained
  - What is TI, why is it used
• Why Threat Intelligence can be Valuable
  - Situational awareness, investigation enrichment, reducing the attack surface
• Criticisms/Limitations of Threat Intelligence
  - Attribution issues, reactive nature, old IOCs, false-positive IOCs
• The Future of Threat Intelligence
  - Tenable Predictive Prioritization (mixing threat intel with vulnerability management data to calculate dynamic risk scores)
• Types of Intelligence
  - SIGINT, OSINT, HUMINT, GEOINT

2: Threat Actors

• Common Threat Agents
  - Cybercriminals, hacktivists, insider threats, nation-states
• Motivations
  - Financial, social, political, other
• Skill Levels/Technical Ability
  - Script Kiddies, Hackers, APTs
• Actor Naming Conventions
  - Animals, APT numbers, other conventions
• Common Targets
  - Industries, governments, organizations

3: Advanced Persistent Threats

• What are APTs?
  - What makes an APT?, Real-world examples of APTs + their operations
• Motivations for Cyber Operations
  - Why APTs do what they do (financial, political, social)
• Tools, Techniques, Tactics
  - What do APTs actually do when conducting operations
• Custom Malware/Tools
  - Exploring custom tools used by APTs, why they're used
• Living-off-the-land Techniques
  - What LOTL is, why it's used, why it can be effectivev

4: Operational Intelligence

• Indicators of Compromise Explained & Examples
  - What IOCs are, how they're generated and shared, using IOCs to feed defences
• Precursors Explained & Examples
  - What precursors are, how they're different from IOCs, how we monitor them
• TTPs Explained & Examples
  - What TTPs are, why they're important, using to maintain defences (preventative)
• MITRE ATT&CK Framework
  - Framework explained and how we map cyber-attacks, real-world example
• Lockheed Martin Cyber Kill Chain
  - Framework explained and how we map cyber-attacks, real-world example
• Attribution and its Limitations
  - Why attribution is hard, impersonation, sharing infrastructure, copy-cat attacks
• Pyramid of Pain
You'll wish we didn't teach you this. It's called the Pyramid of Pain for a reason.

5: Tactical Threat Intelligence

• Threat Exposure Checks Explained
  - What TECs are, how to check your environment for the presence of bad IOCs
• Watchlists/IOC Monitoring
  - What are watchlists, how to monitor for IOCs (SIEM, IDPS, AV, EDR, FW)
• Public Exposure Assessments
  - What PEAs are, how to conduct them, google dorks, harvester, social media
• Open-Web Information Collection
  - How OSINT data is scraped, why it's useful
• Dark-Web Information Collection
  - How intel companies scrape dark web intel, why it's useful, data breach dumps, malicious actors on underground forums, commodity malware for sale
• Malware Information Sharing Platform (MISP)
  - What is MISP, why is it used, how to implement MISP

6: Strategic Threat Intelligence

• Intelligence Sharing and Partnerships
  - Why sharing intel is important, existing partnerships, US-CERT, NCCIC, NCSC, ISACs
• IOC/TTP Gathering and Distribution
• Campaign Tracking & Situational Awareness
  - Why we track actors, why keeping the team updated is important
• New Intelligence Platforms/Toolkits
  - Undertaking proof-of-value demos to assess the feasibility of new tooling
• OSINT vs. Paid-for Sources
  - Threat Intelligence Vendors, Public Threat Feeds, National Vulnerability Database, Twitter

7: Malware and Global Campaigns

• Types of Malware Used by Threat Actors
  - Trojans, RATs, Ransomware, Backdoors, Logic Bombs
• Globally recognized Malware Campaigns
  - Emotet, Magecart, IcedID, Sodinikobi, Trickbot, Lokibot

8: Further Reading

• Further Reading Material
  - Links to more resources that students may find helpful.

Tools exposure provided in the above section:

• AlienVAULT OTX
• MITRE & ATTACK
• MISP
• Maltego
• ONLINE SOURCES

INFOSECTRAIN

sales@infosectrain.com | www.infosectrain.com